
मोबाइल डिवाइस सुरक्षा

भाग 4 आंकलन और मूल्यांकन

Mobile Device Security

Part 4 Assessment and Evaluation

ICS 33.050.10, 35.030

© BIS 2021



भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
मानक भवन, 9 बहादुरशाह ज़फर मार्ग, नई दिल्ली – 110002
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI-110002
www.bis.gov.in www.standardsbis.in

FOREWORD

This Indian Standard (Part 4) was adopted by the Bureau of Indian Standards, after the draft finalized by Information Systems Security and Privacy Sectional committee had been approved by the Electronics and Information Technology Divisional council.

There is no ISO/IEC Standard on this subject.

This standard is one of the series of Indian Standards on Mobile device security. Other parts in this series are:

Part 1 Overview

Part 2 Security requirements

Part 3 Security levels

As mobile based services especially, financial services are gaining popularity, focus on the security of data and content on mobile devices is obvious. Mobile devices need additional protection because their extensive mobility (portability) and always on connectivity (generally using untrusted public network) places them at higher exposure to threats than other client devices such as desktop and laptop devices which are normally used only within the organization's facilities and on the organization's networks.

It requires a totally different approach and strategy to address security of mobile devices as compared to normal computer based systems and applications. Mobile devices uses mobile ecosystem that involves various subsystems and components to provide an environment to enable the operations and connectivity of mobile devices and information systems. Therefore, security of mobile needs to be addressed at different layers (subsystems and components) of the mobile ecosystem covering mobile device technology stack (including firmware, embedded components, operating system, pre-installed applications like mobile browser, device management software agent, VPN client, Email client, etc.), Third party mobile applications, networks and communication interfaces (including cellular, Wi-Fi, Bluetooth, NFC), mobile infrastructure (including mobile app store and services) and enterprise mobile support/monitoring services (enterprise mobility management [EMM]/device management software and mobile application management [MAM]). All these components of the mobile ecosystem shall be considered for defining and assessing the security of mobile devices to meet the common security objectives-confidentiality, integrity and availability.

This series of standards is applicable to the following:

- a) Organizations designing, developing, and manufacturing mobile devices;
- b) Customers seeking confidence in the security of mobile devices used by them;
- c) Organizations seeking confidence in the security of mobile devices used by them; and
- d) Organizations performing security assessment of mobile devices.

In the formulation of this standard, assistance has been derived from the following documents:

NIST Special Publication 1800-4b (Draft) — Mobile Device Security, Approach, Architecture, and Security Characteristics Cloud and Hybrid Builds

NIST Special Publication 800-124 Revision 1; Guidelines for Managing the Security of Mobile Devices in the Enterprise, June 2013

The composition of the Committee and Panel, responsible for the formulation of this standard is given at Annex D.

CONTENTS

	<i>Page No.</i>
0 INTRODUCTION	... 1
1 SCOPE	... 3
2 REFERENCES	... 3
3 TERMINOLGY	... 3
4 APPROACH, METHODOLOGY AND INPUTS REQUIRED FOR SECURITY ASSESSMENT AND EVALUATION	... 3
4.1 General	... 3
4.2 Approach and Methodology	... 5
4.3 Inputs Required	... 6
ANNEX A CHECKLISTS FOR MOBILE OPERATING SYSTEM SECURITY	... 7
ANNEX B CHECKLIST FOR MOBILE PRE-INSTALLED APPLICATION SECURITY	... 9
ANNEX C MOBILE DEVICE SECURITY CONTROL VERIFICATION	... 11
ANNEX D COMMITTEE COMPOSITION	... 13
BIBLIOGRAPHY	... 16

LIST OF TABLES

Table 1	Limited Mobile Device Security Control Requirements for Security Level 1	... 4
Table 2	Mobile Device Security Control Requirements for Security Level 2	... 4
Table 3	Checklist for Mobile Operating System Based on SANS Mobile Device Security Checklist	... 7
Table 4	Checklist for Mobile Operating System based on CIS Google Android Benchmark, v1.2.0-08-06-2018	... 7
Table 5	Checklist for Mobile Operating System based on CIS Apple iOS 12 Benchmark, v1.0.0 - 10-19-2018	... 8
Table 6	Checklist for Mobile Pre-installed Application Security	... 9
Table 7	Mobile Device Security Control Verification	... 11

This page has been intentionally left blank

0 INTRODUCTION

Mobile device consists of a set of components of the mobile technology stack covering mobile device hardware (processor, storage, execution environment); mobile firmware; mobile operating system; and pre-installed (bundled) apps.

A mobile ecosystem is an interconnected, interdependent set of various systems and core components which include mobile device technology stack, mobile network, mobile applications, and vendor mobile infrastructure.

For overall security of mobile device, the security of the mobile device technology stack as well as the security of the mobile device due to mobile ecosystem need to be addressed.

In addition to the security requirements, the mobile devices used for personal and enterprise in different scenario are defined through security levels which need to be assessed and evaluated.

This page has been intentionally left blank

*Indian Standard***MOBILE DEVICE SECURITY****PART 4 ASSESSMENT AND EVALUATION****1 SCOPE**

This standard (Part 4) describes approach and methodology for assessment and evaluation of mobile device security for security levels defined in Part 3 “Security levels” of this standard.

Security assessment and evaluation for two security levels cover mobile OS security; mobile pre-installed application security; and mobile device security controls.

2 REFERENCES

The standards/documents given below contains provisions, which through reference in this text constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards/documents are subject to revision, and parties to agreement based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed as follows:

<i>IS No./Other Publication</i>	<i>Title</i>
IS 17737 (Part 1) : 2021	Mobile device security: Part 1 Overview
IS 17737 (Part 2) : 2021	Mobile device security: Part 2 Security requirements
IS 17737 (Part 3) : 2021	Mobile device security: Part 3 Security levels

CIS Benchmarks (Android and iOS)

OWASP Top 10 Mobile Security Risks, 2016

OWASP MASVS, Version 1.1

SANS Mobile Device Checklist

3 TERMINOLGY

For the purpose of this standard (Part 4) the definitions given in IS 17737 (Part 1) : 2021 shall apply.

4 APPROACH, METHODOLOGY AND INPUTS REQUIRED FOR SECURITY ASSESSMENT AND EVALUATION**4.1 General**

There are two levels of security defined for mobile device in the Part 3 of this standard. These levels are as follows:

- Security Level 1: Baseline Security
- Security Level 2: Comprehensive Security

4.1.1 Security Assessment and Evaluation - Security Level 1

The security level 1 defines the basic security requirements of mobile device. It covers:

- Mobile OS security requirements as given in **6.4.1** of Part 2 of this standard;
- Mobile pre-installed application security requirements as given in **6.4.2** of Part 2 of this standard; and
- Limited mobile device security control requirements as given in Table 1.

Mobile device security controls requirements as given in Table 1 shall be verified

4.1.2 Security Assessment and Evaluation - Security Level 2

The security level 2 is comprehensive security of mobile device. It covers:

- Mobile OS security requirements as given in **6.4.1** of Part 2 of this standard;
- Mobile pre-installed application security requirements as given in **6.4.2** of Part 2 of this standard; and
- Mobile device security control requirements as given in Table 2.

Mobile device security controls requirements as given in Table 2 shall be verified.

Table 1 Limited Mobile Device Security Control Requirements for Security Level 1
(Clause 4.1.1)

Security Characteristics	Security Controls
a) Device protection (device integrity)	1) Application black/whitelisting, 2) Application verification, 3) Verified application and OS updates
b) Data protection	1) Protected storage: i) Device encryption, ii) Remote wipe 2) Protected communications: i) Virtual private network (VPN)
c) Data isolation	3) Device resource management
d) Identity and authorization	1) Local user authentication to applications, 2) Local user authentication to device
e) Monitoring	1) Root and jailbreak detection
f) Privacy protection	1) Informed consent of user, 2) Privacy notification provided to user

Table 2 Mobile Device Security Control Requirements for Security Level 2
(Clause 4.1.2)

Security Characteristics	Security Controls
a) Device protection (device integrity)	1) Baseband integrity checks, 2) Application black/whitelisting, 3) Device integrity checks: i) Boot validation, 4) Application verification, and 5) Verified application and OS updates
b) Data protection	1) Protected storage: i) Device encryption, ii) Secure containers, iii) Trusted key storage, and iv) Remote wipe. 2) Protected communications: i) Virtual private network (VPN), and ii) To include per-App VPN. 3) Data protection in process: i) Encrypted memory, and ii) Trusted execution environment.
c) Data isolation	1) Sandboxing, 2) Memory isolation, 3) Trusted execution environment, 4) Device resource management, and 5) Baseband isolation.
d) Identity and authorization	1) Local user authentication to applications, 2) Local user authentication to device, 3) Remote user authentication, and 4) Credential and token storage and use.
e) Monitoring	1) Auditing and logging, and 2) Root and jailbreak detection.
f) Privacy protection	1) Informed consent of user, and 2) Privacy notification provided to user.

4.2 Approach and Methodology

The mobile OS security requirements and mobile pre-installed application security requirements for security level 1 and 2 are the same. But the mobile device security control requirements are different; at security level 1 only limited mobile device security control requirements are applicable whereas at security level 2 all mobile device security control requirements are applicable.

The assessment and evaluation of these security requirements at security level 1 and 2 are described below:

4.2.1 Mobile Operating System Security Requirements Verification

A mobile operating system is a software, which runs at the highest, privilege level and can directly control hardware resources. The OS handles most user interaction and provides the execution environment for apps. Most mobile operating systems are tied to specific hardware, with little flexibility. A mobile OS is responsible for identifying and defining mobile device features and functions, including application sandbox, Kernel, Media Services, Runtime Environment, etc.

A new mobile device comes with operating system having default configuration setting. In order to make it secure, the default operating system setting needs to be configured with secure settings before use.

The security of the mobile operating system shall be verified by checking its configuration settings using a checklist with focus on security configuration issues that are unique to the mobile platform.

The checklist shall be based on the following security principles (see 6.4.1 of Part 2 of this standard):

- a) Data at rest;
- b) Data in transit protection;
- c) Access control;
- d) Application updates;
- e) Integrity violation checking;
- f) Security updates; and
- g) Verified boot mechanism.

A checklist covering above security principles or following checklists may be used:

- 1) SANS checklist,
- 2) CIS checklist for Android, and
- 3) CIS checklist for iOS.

A checklist for mobile operating system based on SANS & CIS checklists is given in Annex A.

4.2.2 Mobile Pre-installed Application Security Requirements Testing

Pre-installed Application is a software already installed and licensed on a mobile device bought from

an original equipment manufacturer (OEM). The examples include, calendar, calculator, mobile browser, device management software agent, VPN client, Email client, etc.

These pre-installed apps shall be tested as per latest OWASP Top 10 mobile security risks and OWASP Mobile Application Security Verification Standard (MASVS) L1:

- a) Following tests shall be carried out as per OWASP Top 10 mobile security risks:
 - 1) M1: Improper Platform Usage;
 - 2) M2: Insecure Data Storage;
 - 3) M3: Insecure Communication;
 - 4) M4: Insecure Authentication;
 - 5) M5: Insufficient Cryptography;
 - 6) M6: Insecure Authorization;
 - 7) M7: Client Code Quality;
 - 8) M8: Code Tampering;
 - 9) M9: Reverse Engineering; and
 - 10) M10: Extraneous Functionality.
- b) Following tests shall be carried out as per OWASP Mobile Application Security Verification Standard (MASVS) L1:
 - 1) V1: Architecture, Design and Threat Modeling Requirements;
 - 2) V2: Data Storage and Privacy Requirements;
 - 3) V3: Cryptography Requirements;
 - 4) V4: Authentication and Session Management Requirements;
 - 5) V5: Network Communication Requirements;
 - 6) V6: Platform Interaction Requirements; and
 - 7) V7: Code Quality and Build Setting Requirements.

MASVS based checklist is given in Annex B.

4.2.3 Mobile Device Security Control Requirements Verification

The high level security risks and security threats posed to a mobile device (mobile hardware, firmware, mobile OS, and pre- installed Apps) comes from:

- a) Mobile Device based Security Risks (Untrusted Mobile Device);
- b) Mobile Network based Security Risks (Untrusted Network);
- c) Mobile User Behavior based Security Risks (User Behavior and Awareness); and
- d) Malicious Apps and Malware based Security Risks (Untrusted Third Party Applications and malicious Systems).

These security risks and threats to a mobile device can be addressed through a set of Security Characteristics which can be associated with Security Controls.

The methodology for assessment of these security control requirements is based on:

- 1) Verifying the security control mechanisms defined; and
- 2) Implementation of defined security controls in a mobile device.

Verification of the security control mechanisms defined shall be done for its adequacy. This shall be carried out by reviewing the security documentation provided by the device manufacturer.

After verifying the adequacy of security controls defined, implementation of the security control shall be undertaken. This shall be carried out by testing/audit of the security controls.

The testing/audit shall be done using the combination of followings:

- i. Independent testing/audit carried out by independent test lab.
- ii. Demonstration of testing by manufacturer to independent test lab and verification of internal test reports of the mobile device.
- iii. Verification of third party test/audit reports and certificates of the mobile device.
- iv. Verification of the details of components used with part numbers along with sources of supply.

The assessment and evaluation checkpoints for security controls are given in Annex C.

4.3 Inputs Required

4.3.1 Inputs Required for Security Level 1

The following documentation shall be provided by the device manufacturer:

- a) Device details (providing make, model, serial number, operating system, mobile pre-installed applications, location of manufacturing, etc.) submitted for assessment and evaluation.
- b) Mobile device detailed specifications with capabilities and features.

- c) Security policies and practices used for the mobile device.
- d) Implementation details of the security controls identified in Table 1.
- e) Any other document(s) that will provide more insight over the implementation of security.

4.3.2 Inputs Required for Security Level 2

The following documentation shall be provided by the device manufacturer:

- a) Device details (providing make, model, serial number, operating system, mobile pre-installed applications, location of manufacturing, etc.) submitted for assessment and evaluation.
- b) Mobile device detailed specifications with capabilities and features.
- c) Security architecture document covering security design details.
- d) Security policies and practices used for the mobile device.
- e) Implementation details of the security controls identified in Table 2.
- f) Details of components used with part numbers along with sources of supply.
- g) Internal test reports of the mobile device.
- h) Third party test/audit reports and certifications obtained for the mobile device.
- j) Any other document(s) that will provide more insight over the implementation of security.

NOTE — It is expected that the security documentation will specify the implementations required by the Standard. Documentation can be provided in three ways. First option is to provide full comprehensive document explaining the controls completely. Second option is to provide the limited documentation sufficient to provide confidence to the Evaluator regarding the implementation. Third option is to visit the vendor/developer/manufacturer's premises and show the documents pertaining to the controls so that the team of Evaluators gains confidence in the implementation of security controls.

ANNEX A

(Clause 4.2.1)

CHECKLISTS FOR MOBILE OPERATING SYSTEM SECURITY

Table 3 Checklist for Mobile Operating System Based on SANS Mobile Device Security Checklist

Sl. No.	Description
a)	Ability to encrypt information at rest
b)	Supports locks after timeout
c)	Supports unlocking mobile with biometrics or longer passwords (> 4).
d)	Lock or secure security settings so users cannot delete or change mandatory settings
e)	Supports disabling developer access.
f)	Supports disabling third party app store access.
g)	Supports tools to evaluate and uninstall apps with excessive permissions.
h)	Supports installation of OS platform updates.
j)	Supports checking OS versions installed and checking latest available security & patch level.
k)	Supports feature for remote location services for lost.
l)	Supports erasing network settings to forget old networks not in use.
m)	Supports prompting “trust this computer” when plugging mobile to another device/computer.
n)	Supports strong password or two-factor authentication.
p)	Supports disabling auto connect to WiFi networks.

NOTE — It is recommended that latest versions of SANS checklist be referred.

Table 4 Checklist for Mobile Operating System based on CIS Google Android Benchmark, v1.2.0-08-06-2018

A. Android OS Security Settings	
1	Ensure device firmware is up to date
2)	Ensure ‘Screen Lock’ is set to ‘Enabled’
3)	Ensure ‘Make pattern visible’ is set to ‘Disabled’ (if using a pattern as device lock mechanism)
4)	Ensure ‘Automatically Lock’ is set to ‘Immediately’
5)	Ensure ‘Power button instantly locks’ is set to ‘Enabled’
6)	Ensure ‘Lock Screen Message’ is configured
7)	Do not connect to untrusted Wi-Fi networks
8)	Ensure ‘Show passwords’ is set to ‘Disabled’
9)	Ensure ‘Developer Options’ is set to ‘Disabled’
10)	Ensure ‘Install unknown apps’ is set to ‘Disabled’

A. Android OS Security Settings	
11)	Do not root your device
12)	Ensure ‘Smart Lock’ is set to ‘Disabled’
13)	Ensure ‘Lock SIM card’ is set to ‘Enabled’
14)	Ensure ‘Find My Device’ is set to ‘Enabled’
15)	Ensure ‘Automatic date & time’ and ‘Automatic time zone’ are set to ‘Enabled’
16)	Ensure ‘Remotely locate this device’ is set to ‘Enabled’
17)	Ensure ‘Allow remote lock and erase’ is set to ‘Enabled’
18)	Ensure ‘Scan device for security threats’ is set to ‘Enabled’
19)	Ensure ‘Improve harmful app detection’ is set to ‘Enabled’
20)	Ensure ‘Ask for unlock pattern/PIN/password before unpinning’ is set to ‘Enabled’
21)	Ensure ‘Sleep’ is set to ‘1 minute or less’
22)	Ensure ‘Wi-Fi assistant’ is set to ‘Disabled’
23)	Keep device Apps up to date
24)	Ensure ‘Add users from lock screen’ is set to ‘Disabled’
25)	Ensure ‘Guest profiles’ do not exist
26)	Review app permissions periodically
27)	Ensure ‘Instant apps’ is set to ‘Disabled’
B. Android OS Privacy Settings	
1)	Ensure ‘Notifications on the lock screen’ is set to ‘Disabled’
2)	Ensure ‘Location Services’ is set to ‘Disabled’
3)	Ensure ‘Back up to Google Drive’ is ‘Disabled’
4)	Ensure ‘Web and App Activity’ is set to ‘Disabled’
5)	Ensure ‘Device Information’ is set to ‘Disabled’
6)	Ensure ‘Voice and Audio Activity’ is set to ‘Disabled’
7)	Ensure ‘YouTube Search History’ is set to ‘Disabled’
8)	Ensure ‘YouTube Watch History’ is set to ‘Disabled’
9)	Ensure ‘Google Location History’ is set to ‘Disabled’
10)	Ensure ‘Opt out of Ads Personalization’ is set to ‘Enabled’
C. Android OS Chrome Browser Settings	
1)	Ensure ‘Microphone’ is set to ‘Enabled’
2)	Ensure ‘Location’ is set to ‘Enabled’
3)	Ensure ‘Allow third-party cookies’ is set to ‘Disabled’
4)	Ensure ‘Safe Browsing’ is set to ‘Enabled’
5)	Ensure ‘Search and site suggestions’ is set to ‘Disabled’
6)	Ensure ‘Do Not Track’ is set to ‘Enabled’

**Table 5 Checklist for Mobile Operating System
based on CIS Apple iOS 12 Benchmark,
v1.0.0 - 10-19-2018**

A. Benchmark Guidance	
B. Configuration Profile Recommendations for End-User Owned Devices	
1) General	
a)	Ensure a 'Consent Message' has been 'Configured'
b)	Ensure 'Controls when the profile can be removed' is set to 'Always'
2) Restrictions	
a) Functionality	
i.	Ensure 'Allow voice dialing while device is locked' is set to 'Disabled'
ii.	Ensure 'Allow Siri while device is locked' is set to 'Disabled'
iii.	Ensure 'Allow managed apps to store data in iCloud' is set to 'Disabled'
iv.	Ensure 'Force encrypted backups' is set to 'Enabled'
v.	Ensure 'Allow users to accept untrusted TLS certificates' is set to 'Disabled'
vi.	Ensure 'Allow documents from managed sources in unmanaged destinations' is set to 'Disabled'
vii.	Ensure 'Allow documents from unmanaged sources in managed destinations' is set to 'Disabled'
viii.	Ensure 'Treat AirDrop as unmanaged destination' is set to 'Enabled'
ix.	Ensure 'Allow Handoff' is set to 'Disabled'
x.	Ensure 'Force Apple Watch wrist detection' is set to 'Enabled'
xi.	Ensure 'Show Control Center in Lock screen' is set to 'Disabled'
xii.	Ensure 'Show Notification Center in Lock screen' is set to 'Disabled'
b) Apps	
i.	Ensure 'Force fraud warning' is set to 'Enabled'
ii.	Ensure 'Accept cookies' is set to 'From websites I visit' or 'From current website only'
3) Domains	
a)	Ensure 'Managed Safari Web Domains' is 'Configured'
4) Passcode	
a)	Ensure 'Allow simple value' is set to 'Disabled'
b)	Ensure 'Minimum passcode length' is set to '6' or greater
c)	Ensure 'Maximum Auto-Lock' is set to '2 minute' or less
d)	Ensure 'Maximum grace period for device lock' is set to 'Immediately'
e)	Ensure 'Maximum number of failed attempts' is set to '6'
5) VPN	
a)	Ensure 'VPN' is 'Configured'
6) Mail	
a)	Ensure 'Allow user to move messages from this account' is set to 'Disabled'

7) Notifications	
a)	Ensure 'Notification Settings' are configured for all 'Managed Apps'
C. Configuration Profile Recommendations for Institutionally Owned Devices	
1) General	
a)	Ensure 'Controls when the profile can be removed' is set to 'Never'
2) Restrictions	
a) Functionality	
i)	Ensure 'Allow screenshots and screen recording' is set to 'Disabled'
ii)	Ensure 'Allow voice dialing while device is locked' is set to 'Disabled'
iii)	Ensure 'Allow Siri while device is locked' is set to 'Disabled'
iv)	Ensure 'Allow iCloud backup' is set to 'Disabled'
v.	Ensure 'Allow iCloud documents and data' is set to 'Disabled'
vi.	Ensure 'Allow iCloud Keychain' is set to 'Disabled'
vii.	Ensure 'Allow managed apps to store data in iCloud' is set to 'Disabled'
viii.	Ensure 'Force encrypted backups' is set to 'Enabled'
ix.	Ensure 'Allow Erase All Content and Settings' is set to 'Disabled'
x.	Ensure 'Allow users to accept untrusted TLS certificates' is set to 'Disabled'
xi.	Ensure 'Allow installing configuration profiles' is set to 'Disabled'
xii.	Ensure 'Allow adding VPN configurations' is set to 'Disabled'
xiii.	Ensure 'Allow modifying cellular data app settings' is set to 'Disabled'
xiv.	Ensure 'Allow USB accessories while the device is locked' is set to 'Disabled'
xv.	Ensure 'Allow pairing with non-Configurator hosts' is set to 'Disabled'
xvi.	Ensure 'Allow documents from managed sources in unmanaged destinations' is set to 'Disabled'
xvii.	Ensure 'Allow documents from unmanaged sources in managed destinations' is set to 'Disabled'
xviii.	Ensure 'Treat AirDrop as unmanaged destination' is set to 'Enabled'
xix.	Ensure 'Allow Handoff' is set to 'Disabled'
xx.	Ensure 'Force Apple Watch wrist detection' is set to 'Enabled'
xxi.	Ensure 'Allow setting up new nearby devices' is set to 'Disabled'
xxii.	Ensure 'Show Control Center in Lock screen' is set to 'Disabled'
xxiii.	Ensure 'Show Notification Center in Lock screen' is set to 'Disabled'

b) Apps	
i.	Ensure 'Force fraud warning' is set to 'Enabled'
ii.	Ensure 'Accept cookies' is set to 'From websites I visit' or 'From current website only'
3) Domains	
a)	Ensure 'Managed Safari Web Domains' is Configured
4) Passcode	
a)	Ensure 'Allow simple value' is set to 'Disabled'
b)	Ensure 'Minimum passcode length' is set to '6' or greater
c)	Ensure 'Maximum Auto-Lock' is set to '2 minutes' or less
d)	Ensure 'Maximum grace period for device lock' is set to 'Immediately'
e)	Ensure 'Maximum number of failed attempts' is set to '6'
5) VPN	
a)	Ensure 'VPN' is 'Configured'
6) Mail	
a)	Ensure 'Allow user to move messages from this account' is set to 'Disabled'
b)	Ensure 'Allow Mail Drop' is set to 'Disabled'

7) Notifications	
a)	Ensure 'Notification Settings' are configured for all 'Managed Apps'
8) Lock Screen Message	
a)	Ensure 'If Lost, Return to... Message' is 'Configured'
D. Additional Recommendations	
1)	Ensure device is not obviously jailbroken
2)	Ensure 'Software Update' returns 'Your software is up to date.'
3)	Ensure 'Automatic Downloads' of 'App Updates' is set to 'Enabled'
4)	Ensure 'Find My iPhone/iPad' is set to 'Enabled' on end-user owned devices
5)	Ensure the latest iOS device architecture is used by high-value targets

ANNEX B

(Clause 4.2.2)

CHECKLIST FOR MOBILE PRE-INSTALLED APPLICATION SECURITY

Following checklist is adopted from OWASP MASVS, Version 1.1.

Table 6 Checklist for Mobile Pre-installed Application Security

Sl. No.	Description
A. Architecture, Design and Threat Modeling Requirements	
1)	All app components are identified and known to be needed
2)	Security controls are enforced on the client side and the respective remote endpoints
3)	A high-level architecture for the mobile app and all connected remote services has been defined and security has been addressed in that architecture
4)	Data considered sensitive in the context of the mobile app is clearly identified
B. Data Storage and Privacy Requirements	
1)	System credential storage facilities are used appropriately to store sensitive data, such as PII, user credentials or cryptographic keys.
2)	No sensitive data should be stored outside of the app container or system credential storage facilities.
3)	No sensitive data is written to application logs.

Sl. No.	Description
4)	No sensitive data is shared with third parties unless it is a necessary part of the architecture.
5)	The keyboard cache is disabled on text inputs that process sensitive data.
6)	No sensitive data is exposed via IPC mechanisms.
7)	No sensitive data, such as passwords or pins, is exposed through the user interface.
C. Cryptography Requirements	
1)	The app does not rely on symmetric cryptography with hardcoded keys as a sole method of encryption.
2)	The app uses proven implementations of cryptographic primitives.
3)	The app uses cryptographic primitives that are appropriate for the particular use-case, configured with parameters that adhere to industry best practices.
4)	The app does not use cryptographic protocols or algorithms that are widely considered deprecated for security purposes.
5)	The app doesn't re-use the same cryptographic key for multiple purposes.
6)	All random values are generated using a sufficiently secure random number generator.

Sl. No.	Description
D. Authentication and Session Management Requirements	
1)	If the app provides users access to a remote service, some form of authentication, such as username/password authentication, is performed at the remote endpoint.
2)	If stateful session management is used, the remote endpoint uses randomly generated session identifiers to authenticate client requests without sending the user's credentials.
3)	If stateless token-based authentication is used, the server provides a token that has been signed using a secure algorithm.
4)	The remote endpoint terminates the existing session when the user logs out.
5)	A password policy exists and is enforced at the remote endpoint.
6)	The remote endpoint implements a mechanism to protect against the submission of credentials an excessive number of times.
E. Network Communication Requirements	
1)	Data is encrypted on the network using TLS. The secure channel is used consistently throughout the app.
2)	The TLS settings are in line with current best practices, or as close as possible if the mobile operating system does not support the recommended standards.
3)	The app verifies the X.509 certificate of the remote endpoint when the secure channel is established. Only certificates signed by a trusted CA are accepted.
F. Platform Interaction Requirements	
1)	The app only requests the minimum set of permissions necessary.
2)	All inputs from external sources and the user are validated and if necessary sanitized. This includes data received via the UI, IPC mechanisms such as intents, custom URLs, and network sources.
3)	The app does not export sensitive functionality via custom URL schemes, unless these mechanisms are properly protected.

Sl. No.	Description
4)	The app does not export sensitive functionality through IPC facilities, unless these mechanisms are properly protected.
5)	Java Script is disabled in Web Views unless explicitly required.
6)	Web Views are configured to allow only the minimum set of protocol handlers required (ideally, only https is supported). Potentially dangerous handlers, such as file, tel and app-id, are disabled.
7)	If native methods of the app are exposed to a WebView, verify that the WebView only renders JavaScript contained within the app package.
8)	Object deserialization, if any, is implemented using safe serialization APIs.
G. Code Quality and Build Setting Requirements	
1)	The app is signed and provisioned with a valid certificate, of which the private key is properly protected.
2)	The app has been built in release mode, with settings appropriate for a release build (for example, non-debuggable).
3)	Debugging symbols have been removed from native binaries.
4)	Debugging code has been removed, and the app does not log verbose errors or debugging messages.
5)	All third-party components used by the mobile app, such as libraries and frameworks, are identified, and checked for known vulnerabilities.
6)	The app catches and handles possible exceptions.
7)	Error handling logic in security controls denies access by default.
8)	In unmanaged code, memory is allocated, freed and used securely.
9)	Free security features offered by the toolchain, such as byte-code minification, stack protection, PIE support and automatic reference counting, are activated.

ANNEX C

(Clause 4.2.3)

MOBILE DEVICE SECURITY CONTROL VERIFICATION

Table 7 Mobile Device Security Control Verification

Security Characteristics	Security Controls Requirements	Inputs Required	Assessment and Evaluation Checkpoints
a) Device protection (device integrity)	1) Baseband integrity checks	Details of chip set/baseband processor used in the mobile device.	Check the part number of the chip set/processor used and its specifications from OEM's Specification Sheet/Website. Verify that the chip set/ processor is used by the mobile device and has integrity checking feature – manufacturer to demonstrate.
	2) Application black/whitelisting	Details of application black/whitelisting mechanism used in the mobile device.	Check the availability of the App black/whitelisting feature in the mobile device. Assess the feature – manufacturer to demonstrate.
	3) Device integrity checks: Boot validation	Device integrity checks - Boot process details of the mobile device.	Check whether mobile device has this feature and it is functioning – manufacturer to demonstrate.
	4) Application verification	Details of application verification mechanism used in the mobile device.	Check that the capability to verify application source before it is installed exists and verify the same – manufacturer to demonstrate.
	5) Verified application and OS updates	Details of application and OS update verification mechanism used in the mobile device.	Check that the capability to verify application and OS update source before it is installed exists and verify the same – manufacturer to demonstrate.
b) Data protection	1) Protected storage:	---	Check if device has capability to protect data in storage.
	i) Device encryption	What type of encryption is used by device and its details along with certification, if any.	Check what encryption is used by the device and it is adequate and certified. Verify that the data in storage on device is actually encrypted – manufacturer to demonstrate.
	ii) Secure containers	Details of containerization feature used by the device.	Check that device has containerization capability. Verify that containerization is used by the device and is secure – manufacturer to demonstrate.
	iii) Trusted Key Storage	Details of storing the trusted keys	Check that device securely stores the trusted keys and it is effective – manufacturer to demonstrate.
	iv) Remote wipe	Details of remote wipe feature or any other safe guards used for protecting the data remotely.	Check the mechanism used for remote protection of data such as remote wipe. Verify that the same has been implemented and it is effective – manufacturer to demonstrate.
	2) Protected communications:	---	Check if device has capability to protect data in transit.
	i) Virtual private network (VPN)	Details of protecting confidentiality and integrity of information in transit using VPN/ cryptography.	Check the mechanism used protecting confidentiality and integrity of information in transit such as VPN/ cryptography. Verify that the same has been implemented and it is effective - manufacturer to demonstrate.
	ii) To include per-App VPN	Details of per App VPN used in the device	Check per App VPN mechanism defined. Verify that the same has been implemented and it is effective – manufacturer to demonstrate.
	3) Data protection in Process:	–	Check if device has capability to protect data in processing.
	i) Encrypted memory	Details of encrypted memory used in the device	Check mechanism used for encrypted memory. Verify that the same has been implemented and it is effective – manufacturer to demonstrate.
	ii) Trusted execution environment	Details of the trusted execution environment used in the device.	Check mechanism used for protecting execution environment. Verify that the same has been implemented and it is effective – manufacturer to demonstrate. Device manufacturer to write APIs to communicate with TEE as per requirements.

Security Characteristics	Security Controls Requirements	Inputs Required	Assessment and Evaluation Checkpoints
c) Data isolation	1) Sandboxing	Details of sandboxing feature used by the device.	Check that device has sandboxing capability. Verify that sandboxing is used by the device and is effective – manufacturer to demonstrate.
	2) Memory isolation	Details of memory isolation feature used by the device.	Check that device has memory isolation capability. Verify that memory isolation is used by the device and is secure – manufacturer to demonstrate.
	3) Trusted execution environment	Details of the trusted execution Environment used by the device.	Check mechanism used for trusted execution environment. Verify that the same has been implemented and it is effective – manufacturer to demonstrate.
	4) Device resource management	Details of the device resource management feature used by the device.	Check mechanism used for device resource management and features. Verify that the same has been implemented – manufacturer to demonstrate.
	5) Baseband isolation	Details of baseband isolation used in the mobile device.	Check mechanism used for baseband isolation. Verify that the same has been implemented and it is effective – manufacturer to demonstrate.
d) Identity and authorization	1) Local user authentication to applications	Details of local user authentication to applications feature used in the mobile device.	Check mechanism used for local user authentication to applications. Verify that the same has been implemented & it is effective – manufacturer to demonstrate.
	2) Local user authentication to device	Details of local user authentication to device feature used in the mobile device.	Check mechanism used for local user authentication to device. Verify that the same has been implemented and it is effective – manufacturer to demonstrate.
	3) Remote user authentication	Details of remote user authentication feature used in the mobile device.	Check mechanism used for remote user authentication. Verify that the same has been implemented and it is effective – manufacturer to demonstrate.
	4) Credential and token storage and use	Details of credential and token storage and its usage in the mobile device.	Check mechanism used for credential and token storage and use. Verify that the same has been implemented and it is effective – manufacturer to demonstrate.
e) Monitoring	1) Auditing and logging	Details of auditing and logging feature used in the mobile device.	Check mechanism used for auditing and logging. Verify that the same has been implemented – manufacturer to demonstrate.
	2) Root and jailbreak detection	Details of root and jailbreak detection feature used in the mobile device.	Check mechanism used for root and jailbreak detection. Verify that the same has been implemented and it is effective – manufacturer to demonstrate.
f) Privacy protection	1) Informed consent of user	Details of informed consent of user feature used in the mobile device.	Check mechanism used for informed consent of user. Verify that the same has been implemented and it is effective – manufacturer to demonstrate.
	2) Privacy notification provided to user	Details of privacy notification provided to user feature used in the mobile device.	Check mechanism used for privacy notification provided to user. Verify that the same has been implemented and it is effective – manufacturer to demonstrate.

ANNEX D*(Foreword)***COMMITTEE COMPOSITION**

Information System Security and Privacy Sectional Committee, LITD 17

<i>Organization</i>	<i>Representative (s)</i>
Ministry of Electronics and Information Technology, New Delhi	SHRI ARVIND KUMAR (Chariman)
Bharat Electronics Limited, Bengaluru	Ms SANGEETHA MANGAL SHRI DEVESH KUMAR SINGH (<i>Alternate</i>)
Centre for Development of Advanced Computing, Pune	DR M. SASI KUMAR SHRIMATI P. R. LAKSHMI ESWARI (<i>Alternate</i>)
Centre for Internet and Society, Bengaluru	SHRI SUNIL ABRAHAM SHRI AMBER SINHA (<i>Alternate I</i>) SHRI GURSHABHAD GROVER (<i>Alternate II</i>)
Confederation of Indian Industry, New Delhi	COL SUHAIL ZAIDI SHRI RAMESH KARWANI (<i>Alternate</i>)
Data Security Council of India, Noida	SHRI ADITYA
Defence Research Development Organization, Ministry of Defence, New Delhi	Ms NOOPUR SHROTRIYA SHRI G. ANIL (<i>Alternate</i>)
HCL, Noida	SHRI SANJEEV CHHABRA
ISI Calcutta	PROF BIMAL ROY
Indian Cellular and Electronics Association, New Delhi	SHRI RAJESH SHARMA Ms ARPITA DE (<i>Alternate</i>)
Indian Institute of Technology Madras, Chennai	PROF ANIL PRABHAKAR
Infosys Technologies Limited, Bengaluru	SHRI SRINIVAS POOSARLA SHRI RAJEEV THYKATT (<i>Alternate I</i>) Ms ASWATHY ASOK (<i>Alternate II</i>)
KCPL	DR V. K. KANHERE
Lady Shri Ram College for Women, New Delhi	Ms SUSHILA MADAN
Larsen and Toubro Limited, Mumbai	SHRI N. SATHYAN SHRI TIRUMALA RAO K. (<i>Alternate</i>)
Ministry of Electronics and Information Technology, New Delhi	SHRI S. K. NEHRA SHRI RAKESH MAHESHWARI (<i>Alternate I</i>) SHRI SANTOSH SONI (<i>Alternate II</i>) DR SOMNATH CHANDRA (<i>Alternate III</i>) SHRI TARUN PANDEY (<i>Alternate IV</i>)
Ministry of Science and Technology, Department of Science & Technology, New Delhi	SHRI SUJIT BANERJEE DR RAJEEV SHARMA (<i>Alternate</i>)
Narnix Technolabs Private Limited, New Delhi	SHRI KISHOR N. NARANG
National Accreditation Board for Certification Bodies, New Delhi	SHRI A. S. BHATNAGAR Ms ANAJNA JAIN (<i>Alternate</i>)
National Payments Corporation of India, Mumbai	MR SATYA KANUNGO SHRI SATEESH PALAGIRI (<i>Alternate</i>)
Oxygen Consulting Services Private Limited, Pune	SHRI SANJIV KUMAR AGARWALA SHRI SACHIN PRAKASH JADHAV (<i>Alternate</i>)
Patanjali Associates Private Limited, New Delhi	SHRI KANTI MOHAN RUSTOGI

IS 17737 (Part 4) : 2021

<i>Organization</i>	<i>Representative (s)</i>
Qualcomm India Private Limited, Bengaluru	DR VINOSH BABU JAMES
Reserve Bank Information Technology Private Limited, Mumbai	SHRI PRASHANT LOTLIKAR SHRI DEEPNARAYAN TIWARI (<i>Alternate</i>)
Smart Chip Private Limited, Noida	MS NISHA CHAUHAN SHRI PANKAJ AGARWAL (<i>Alternate I</i>) SHRI ANKIT GUPTA (<i>Alternate II</i>)
Standardization Testing and Quality Certification (STQC)	SHRI A. K. SHARMA SHRI A. K. UPADHYAYA (<i>Alternate I</i>) SHRI NAKUL AGGRWAL (<i>Alternate II</i>)
Tata Consultancy Services Limited, Mumbai	SHRI SATEESH SRINIWSAIAH SHRI NATARAJAN SWAMINATHAN (<i>Alternate I</i>) SHRI ABHIK CHAUDHURI (<i>Alternate II</i>) SHRI ANUPAM AGRAWAL (<i>Alternate III</i>)
Telecommunication Engineering Center, New Delhi	SHRI S. SRIDHAR SHRI ARVIND CHAWLA (<i>Alternate</i>)
The Perspective, New Delhi	SHRI RAHUL SHARMA
WYSE Biometrics System Private Limited, Pune	SHRI YOGENDRA D. WADASKAR
In personal capacity	SHRIMATI AMUTHA ARUNACHALAM
In personal capacity, Kolkata	DR GARGI KEENI
BIS Directorate General	SHRIMATI REENA GARG, SCIENTIST 'F' AND HEAD (LITD) [REPRESENTING DIRECTOR GENERAL (<i>Ex-officio</i>)]

Member Secretary

SHRI KSHITIJ BATHLA
SCIENTIST 'C' (LITD), BIS

Mobile Security Standards Panel, LITD 17 P4

<i>Organization</i>	<i>Representative(s)</i>
Standardization Testing and Quality Certification (STQC)	SHRI A. K. UPADHYAYA (<i>Convener</i>)
Telecommunication Engineering Center, New Delhi	SHRI P. K. SINGH (<i>Co-Convener</i>)
Apple India Private Limited, Bengaluru	MR JUNAID A. SIDDIQUEE
Cellular Operators Association of India, New Delhi	SHRI ROHIT SINGH
Fime India, Bengaluru	SHRI ANGAJ BHANDARI SHRI HARDIK MIRANI (<i>Alternate</i>)
Google India, Bengaluru	MS TUHINA JOSHI
HCL, Noida	SHRI SANJEEV CHHABRA
Indian Cellular and Electronics Association, New Delhi	SHRI RAJESH SHARMA SHRI TARON MOHAN (<i>Alternate</i>)
KCPL	DR V. K. KANHERE
Pavone Technologies, New Delhi	SHRI ABHINAV SHARMA
Samsung India, Gurugram	SHRI BAPPA MONDAL SHRIMATI NOOR KHAN (<i>Alternate</i>)
Sony India, Mathura	SHRI MANOJ KUMAR GUPTA
Transsion India Limited, Noida	SHRI RAHUL GAUR SHRI VINOD KUNDRA (<i>Alternate</i>)
UL India Private Limited, Bengaluru	SHRI ASHISH MATHUR SHRI AJAY JAIDKA (<i>Alternate</i>)
VIVO Mobile India Private Limited, Delhi	SHRI PAIGHAM DANISH
Vincular Testing Labs India Private Limited, Bengaluru	SHRI VISHAL TOMAR SHRI SACHIN DHIR (<i>Alternate</i>)
Xiaomi Corporation, Bengaluru	MS SURBHI JAIN SHRI MANISH JAIN (<i>Alternate</i>)

BIBLIOGRAPHY

- 1) https://www.cisecurity.org/benchmark/google_android/ for Android OS
- 2) https://www.cisecurity.org/benchmark/apple_ios/ for iOS
- 3) <https://www.sans.org/score/checklists/mobile-device>

This page has been intentionally left blank

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act, 2016* to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Copyright

BIS has the copyright of all its publications. No part of these publications may be reproduced in any form without the prior permission in writing of BIS. This does not preclude the free use, in the course of implementing the standard, of necessary details, such as symbols and sizes, type or grade designations. Enquiries relating to copyright be addressed to the Director (Publications), BIS.

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the latest issue of 'BIS Catalogue' and 'Standards: Monthly Additions'.

This Indian Standard has been developed from Doc No.: LITD 17 (14999).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters:

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110002
Telephones: 2323 0131, 2323 3375, 2323 9402

Website: www.bis.gov.in

Regional Offices:

Telephones

Central	: Manak Bhavan, 9 Bahadur Shah Zafar Marg NEW DELHI 110002	{ 2323 7617 2323 3841
Eastern	: 1/14 C.I.T. Scheme VII M, V.I.P. Road, Kankurgachi KOLKATA 700054	{ 2337 8499, 2337 8561 2337 8626, 2337 9120
Northern	: Plot No. 4-A, Sector 27-B, Madhya Marg CHANDIGARH 160019	{ 265 0206 265 0290
Southern	: C.I.T. Campus, IV Cross Road, CHENNAI 600113	{ 2254 1216, 2254 1442 2254 2519, 2254 2315
Western	: Manakalaya, E9 MIDC, Marol, Andheri (East) MUMBAI 400093	{ 2832 9295, 2832 7858 2832 7891, 2832 7892

Branches : AHMEDABAD. BENGALURU. BHOPAL. BHUBANESHWAR. COIMBATORE.
DEHRADUN. DURGAPUR. FARIDABAD. GHAZIABAD. GUWAHATI.
HYDERABAD. JAIPUR. JAMMU. JAMSHEDPUR. KOCHI. LUCKNOW.
NAGPUR. PARWANOO. PATNA. PUNE. RAIPUR. RAJKOT. VISAKHAPATNAM.

Published by BIS, New Delhi